UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of The Person Boris Castro	)	Case No. 2:24-MJ-03980

AMENDED SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference[and attached hereto].

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

You must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

Date and time issued: July 15, 2024 3:40 PM

Judge's signature

City and state: Los Angeles, CA

Hon. Steve Kim, U.S. Magistrate Judge
Printed Name and Title

AUSA: Dennis Mitchell, Ext. 2484

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:24-MJ-03980	Date and time warrant executed: 7/16/2024 at 09:45 AM	Copy of warrant and inventory left with: Boris CASTRO

Inventory made in the presence of: Special Agent Christin Cichosz

Inventory of the property taken and name of any person(s) seized:

One Samsung Galaxy cellular telephone associated with phone number 213-924-4420.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/23/2024

Executing officer's signature

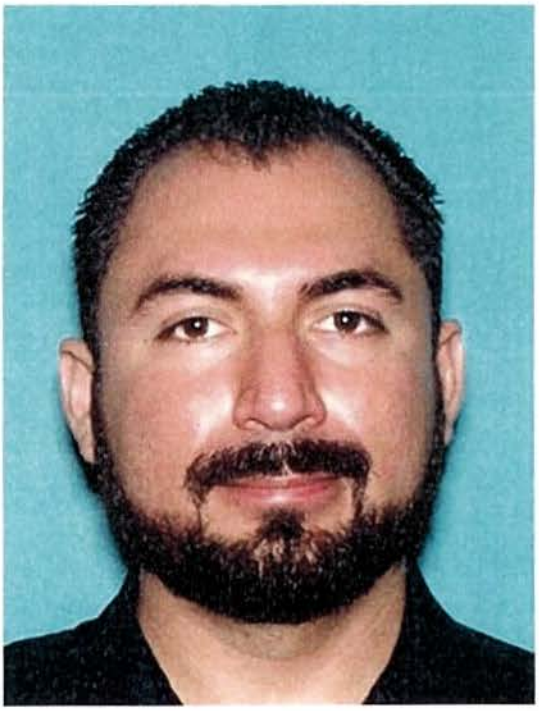
Greg Bazley, Special Agent

Printed name and title

ATTACHMENT A-1

PERSON TO BE SEARCHED

The Person of Boris Castro, further described as a white male, approximately 5'7" tall, weighing 165 pounds, and California Driver's License Y2351811. Below is a picture from his California Driver's License.



The search of the aforementioned person shall include all digital devices, clothing, and personal belongings including backpacks, wallets, briefcases, and bags that are within Boris Castro's immediate vicinity and control.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 42 U.S.C § 6928(d)(2)(A) (treatment, storage, or disposal of a hazardous waste without a permit), and 42 U.S.C § 6928(d)(5) (transportation of a hazardous waste without a manifest) for the period from November 4, 2022, up to and including the date of issuance of this warrant, and are limited to records, information, materials, electronic records, communications, and data such as emails, text messages, chats and chat logs from various third-party applications, images, audio files, videos, and location data:

a. tending to indicate effort to transport and/or dispose of hazardous waste;

b. containing images of hazardous waste;

c. tending to indicate contact with individuals regarding the location(s) at which the hazardous waste might be located, transported, or disposed of;

d. tending to identify electronic media accounts-such as email addresses, IP addresses, social media accounts and phone numbers used to facilitate the transport and/or disposal of hazardous waste;

e. tending to identify co-conspirators, criminal associates or others involved in transporting and/or disposing of hazardous waste;

f. tending to identify travel to of presence at locations involved in transporting and/or disposing of hazardous waste;

g. tending to identify proceeds and/or payments associated with the transport and/or disposal of hazardous waste;

h. tending to identify information regarding the legal requirements applicable to the transport and/or disposal of hazardous waste;

i. tending to indicate permits and official authorization to transport, treat or dispose of hazardous waste;

j. tending to identify the user of, or persons with control over or access to, the telephone; and

k. tending to place in context, identify the creator or receipt of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof. The term "digital device" includes the cell phone belonging to CASTRO known to be a Samsung Galaxy, associated with phone number 213-924-4420.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information that Internet Protocol addresses use by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "application," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The United States will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, under the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the United States will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the United States may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the United States may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The United States may also retain a digital device if the United States, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the United States has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the United States shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained under this warrant may be conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the United States, attorney support staff, and technical experts. Under this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress CASTRO's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of CASTRO's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain

access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices under the authority conferred by this warrant and do not apply to any search of digital devices under any other court order.